INTERNET POLICY REVIEW
Journal on internet regulation

Cryptoeconomics
Volume 10 **Issue** 2

GLOSSARY ENTRY

OPEN ACCESS

PEER REVIEWED

Cryptoeconomics

Jaya Klara Brekke *Durham University* j.k.brekke@durham.ac.uk
Wassim Zuhair Alsindi *Massachusetts Institute of Technology* wassim@pllel.com

DOI: https://doi.org/10.14763/2021.2.1553

Published: 20 April 2021
Received: 18 November 2020 **Accepted:** 27 November 2020

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Brekke, J. K. & Alsindi, W. Z. (2021). Cryptoeconomics. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1553

Keywords: Cryptocurrency, Economics

Abstract: Cryptoeconomics describes an interdisciplinary, emergent and experimental field that draws on ideas and concepts from economics, game theory and related disciplines in the design of peer-to-peer cryptographic systems. Cryptoeconomic systems try to guarantee certain kinds of information security properties using incentives and/or penalties to regulate the distribution of efforts, goods and services in new digital economies. Cryptoeconomics is an embryonic field at present and can be taken to include several areas of focus: information security engineering, mechanism design, token engineering and market design. This portmanteau of cryptography and economics raises questions regarding the epistemic novelty of cryptoeconomics, as distinct from its constituent components.

This article belongs to the **Glossary of decentralised technosocial systems**, a special section of *Internet Policy Review*.

Definition

Cryptoeconomics describes an interdisciplinary, emergent and experimental field that draws on ideas and concepts from economics, game theory and related disciplines in the design of peer-to-peer cryptographic systems. Cryptoeconomic systems try to guarantee certain kinds of information security properties using incentives and/or penalties to regulate the distribution of efforts, goods and services in new digital economies.

Cryptoeconomics is an embryonic field at present and can be taken to include several areas of focus: information security engineering, mechanism design, token engineering and market design. This portmanteau of cryptography and economics raises questions regarding the epistemic novelty of cryptoeconomics, as distinct from its constituent components.

Origin

The term *cryptoeconomics* entered casual usage in the formative years of the Ethereum developer community in 2014-5. The phrase is typically attributed to Vitalik Buterin with the earliest public usage being in a 2015 talk by Vlad Zamfir entitled “What is Cryptoeconomics” (Zamfir, 2015). For Buterin, the aim of cryptoeconomics is “as a methodology for building systems that try to guarantee certain kinds of information security properties" (Buterin, 2017, pp. 46-56). While for Zamfir, the focus is more broadly on the distribution of efforts, goods and services in new digital economies: "A formal discipline that studies protocols that govern the production, distribution, and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols" (Zamfir, 2015, 00:00:58). The term is uncommon amongst Bitcoin developers, but is occasionally used to discuss adversarial scenarios such as state-sponsored defensive mining and transaction censorship (Voskuill, 2018).

Cryptoeconomics was coined by the Ethereum community but was initially inspired by the use of economic incentives in the Bitcoin protocol (Nakamoto, 2008). Bitcoin mining is designed with the intention that it would be more profitable and attractive to contribute to the network than to attack it. With the development of

Ethereum as the first successful general-purpose blockchain protocol, the idea of using economic incentives was also generalised as an approach to achieve a broad variety of behavioural and information security outcomes for decentralised systems. This has led to experimentation with the use of cryptographic techniques and incentives in organisational, financial, market and monetary experiments (Davidson et al., 2016; Halaburda et al., 2018; Voshmgir, 2019).

Motivation for the development of cryptoeconomics arises from the need to solve specific information security, organisational and economic problems that manifest in cryptographic systems. Examples include incentive alignment between stakeholder participants in permissionless networks and developing viable alternative approaches to distributed consensus other than proof-of-work, which is also commonly referred to as blockchain mining. In this sense, the portmanteau cryptoeconomics (or crypto-economics) as a combination of cryptography and economics raises an interesting question regarding epistemic reducibility. Can cryptoeconomics be fully deconvoluted—in other words, retro-synthesised—into its constituent namesakes; is it a mere combination or greater than the sum of its parts? A particular respondent's answer might fall along the lines of their proclivity towards general-purpose blockchain networks and / or proof-of-work.

The aforementioned affinity to *decentralisation* as an axiomatic aim and primary concept originates from a longer history of the development of peer-to-peer systems as a means to establish autonomous networks (Brekke, 2020). With the invention of Bitcoin, economic ideas were added to the toolbox of computer engineers developing leaderless systems. For some, the motivation was to enable economic autonomy and fair distribution of efforts and rewards within such decentralised networks, what scholar of money and the internet Swartz calls *infrastructural mutualism*. For others, the promise of provably scarce and unforgeable virtual commodities—*digital metallism*—was the main attraction (Swartz, 2018). Adherents to the digital metallist ideology often draw upon economic and monetary concepts typically associated with libertarianism and the US far right (Golumbia, 2016).

Evolution

Over time there has been a broadening in the scope of what can be considered *cryptoeconomics* as the variety of consensus systems and token types has proliferated. The different approaches to cryptoeconomics are beginning to settle into distinct layers of a cryptoeconomic 'stack': 'layer 1' referring to the information security of a network protocol such as proof-of-work and proof-of-stake; and 'layer 2' referring to the token, market or mechanism capacities offered by emerging cryptoe-

conomic platforms (Alsindi, 2019).

In recent years a number of networks affording general-purpose computation with facile smart contracting and token creation capabilities have emerged. This layer 2 cryptoeconomics entails the creation of notionally valuable economic assets without being connected to the underlying security properties of the network substrate; for example ERC20-type Ethereum tokens, Non-Fungible Tokens (NFTs) and more recently *Decentralised Finance* (DeFi) synthetic tokens. Whilst having notional economic value, these assets provide negligible security benefits to the base layer of the network: the abstracted non-native assets of 'layer 2' may increase the incentive to attack 'layer 1', as has been discussed in relation to ledger forks (Alsindi, 2019), Initial Coin Offering launches and sudden market-moving events are seen regularly in the hyper financialised DeFi sector (Daian et al., 2019).

The scope and definition of cryptoeconomics is still undergoing *epistemic formation* (0x Salon & Alsindi, 2020) and thus entails specific areas of focus:

Information security engineering: Where the primary focus of the cryptoeconomic endeavour is on the security properties for peer-to-peer 'layer 1' protocols.

Mechanism design: Where the focus is specifically on the use of incentives for behavioural engineering of *rational agents* in a game theoretical setting (Brown-Cohen et al., 2018).

Token engineering: Where the primary focus is on the functionality and properties exhibited by tokens used in a system. Tokens might for example grant token holders specific rights (such as service access or voting privileges as commonly encountered with the ERC-20 pseudo-standard), be *fungible* or *non-fungible* such as NFTs, be generated and distributed through mining, or through *airdrops*. Different token designs are understood to encourage different types of behaviours and organisational properties (Voshmgir, 2019).

Market design: Where the focus is on employing blockchain protocols and tokens in order to experiment with new kinds of markets that generate specific types of outcomes. For example, *bonding curves* determine the price of tokens depending on the supply or other factors, with an aim to influence the behaviour of investors (Titcomb, 2019).

Issues currently associated with the term

Cryptoeconomics is generally understood to combine cryptographic techniques

and economics. However, much of the field of cryptoeconomics *"shows an interesting but also alarming characteristic: its underlying economics is remarkably conventional and conservative"* (Virtanen et al., 2018). Out of the long-standing and broad fields of economics and associated fields of political economy, monetary theory, finance and social study of finance, most literature on cryptoeconomics takes an overly formalist approach to the contested field of game theory (Green & Viljoen, 2020). Virtanen et al. (2018, n.p.) quote a revealing tweet from the influential Nick Szabo: *"An economist or programmer who hasn't studied much computer science, including cryptography, but guesses about it, cannot design or build a long-term successful cryptocurrency. A computer scientist and programmer who hasn't studied much economics, but applies common sense, can."* This means that the potential of cryptoeconomic approaches may be more reformist than revolutionary; *"in spite of their noble intentions, these projects do not in fact break with the current financial paradigm"* (Lotti, 2016, p. 105).

More recent characterisations of cryptoeconomics take a broader societal outlook, for example focusing on the economics of new organisational forms (Davidson et al., 2016), the design of *economic space* (Virtanen et al., 2018), or on economic and monetary design that draws on mutual credit systems (Brock et al., 2018) and *commons* approaches (De Filippi & Hassan, 2015; Catlow, 2019). There is, in other words, much broader economic experimentation taking place with and through peer-to-peer cryptographic systems, however, those explicitly labelled *cryptoeconomic* often imply narrow and formalist approaches limited to Austrian school economics, right wing monetary ideas and game theory, especially apparent in the usage of the term in reference to Bitcoin (Golumbia, 2016; Voskuill, 2018).

One of the ongoing challenges encountered in cryptoeconomics is inherent to *mechanism design* and *market design* economics more generally (Ossandón, 2019). Namely the contradiction between the promise of deterministic outcomes in theory and the complex, emergent behaviours and effects of the systems in real deployments. On the one hand, the market design approach in cryptoeconomics promises to deliver specific properties (information security or behavioural outcomes). But on the other hand, the simple rules of the systems designs produce complexity and unintended outcomes (Voshmgir & Zargham, 2019). A contradiction off-handedly commented on by Ethereum developer Floersch when discussing the Casper proof-of-stake approach: *"[W]e have this complex behavior emerging from really simple economic rules, and this actually not specific to Casper by any means, this is any protocol that are messing around with economics"* (Floersch, 2017, pp. 12-18).

This contradiction—of emergent complexity and unintended effects—is neverthe-

less "productive" for those seeking to promote economic approaches to social problems: the promise of deterministic outcomes makes the models convincing and attractive from a formalist perspective (Green & Viljoen, 2020), while the complexity obscures any "failures" of the design (Nik-Khah & Mirowski, 2019). These shortcomings are instead relegated to being a problem "of the social" or "with humans" or that the implementation was not sufficiently faithful to the protocol, or even that the protocol implementation was not being expansive or radical enough. This contradiction is extensively covered in political economic and economic history and comprises one of the main critiques of the Austrian school of economics in particular (Mirowski & Nik-Khah, 2018; Heilbroner, 1998), what is also called the *performative* aspects of economics. From an information security perspective, the incorporation of economic incentives into protocol design in this sense radically increases the complexity of peer-to-peer systems, and correspondingly also leads to an increased attack surface and wider variety of hypothetical vulnerabilities (Alsindi, 2019).

Conclusion

In summary, cryptoeconomics refers to an emerging field that employs economic concepts in the design of peer-to-peer cryptographic systems. The origins of the field lie in specific information security problems arising out of such systems. Competing approaches draw from a much wider field of economic and political economic thinking, including mutual credit systems and commons frameworks, in order to address questions of organisation and societal outcomes more broadly.

References

0x Salon, & Alsindi, W. Z. (2020). *0x002 Report: Trespasser Theory: Aside on Cryptoeconomic Systems—A case study in attempted epistemic formation?* [Report]. 0x Salon. https://doi.org/10.21428/49968aaa.9160a130#aside-on-cryptoeconomic-systems---a-case-study-in-attempted-epistemic-formation

Alsindi, W. Z. (2019). *TokenSpace: A Conceptual Framework for Cryptographic Asset Taxonomies*. Parallel Industries. https://doi.org/10.21428/0004054f.ccff3c19

Brekke, J. K. (2020). Hacker-engineers and Their Economies: The Political Economy of Decentralised Networks and 'Cryptoeconomics'. *New Political Economy*. https://doi.org/10.1080/13563467.2020.1806223

Brock, A., Atkinson, D., Friedman, E., Harris-Braun, E., Mcguire, E., Russell, J. M., Perrin, N., Luck, N., & Harris-Braun, W. (2017). *Holo Green Paper* [White Paper]. Holo. https://files.holo.host/2017/12/Holo-Green-Paper.pdf

Brown-Cohen, J., Narayanan, A., Psomas, C., & Weinberg, S. M. (2018). Formal Barriers to Longest-Chain Proof-of-Stake Protocols. *ArXiv*. https://arxiv.org/abs/1809.06528

Buterin, V. (2017). *Introduction to Cryptoeconomics, Ethereum Foundation* [Talk]. https://youtu.be/pKqdjaH1dRo

Catlow, R. (2019). Decentralisation and Commoning the Arts. *Free/Libre, Technologies, Arts and the Commons. Unconference Proceedings*, 50–55. http://www.unrf.ac.cy/files/unconference-proceedings-phygital.pdf#page=50

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2019). Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. *ArXiv*. https://arxiv.org/abs/1904.05234

Davidson, S., De Filippi, P., & Potts, J. (2016). *Economics of Blockchain*. https://doi.org/10.2139/ssrn.2744751

De Filippi, P., & Hassan, P. (2015). Measuring Value in the Commons-Based Ecosystem: Bridging the Gap Between the Commons and the Market. In G. Lovink, N. Tkacz, & P. De Vries (Eds.), *MoneyLab Reader: An Intervention in Digital Economy* (pp. 74–91). Institute of Network Cultures. https://networkcultures.org/wp-content/uploads/2015/04/MoneyLab_reader.pdf#page=76

Floersch, K. (2017). *Casper Proof of Stake* [Talk]. Cryptoeconomics and Security Conference, Berkeley. https://youtu.be/ycF0WFHY5kc.

Golumbia, D. (2016). *The politics of Bitcoin. Software as right-wing extremism*. University of Minnesota Press.

Green, B., & Viljoen, S. (2020). Algorithmic Realism: Expanding the Boundaries of Algorithmic Thought. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT '20)*, 19–31. https://doi.org/10.1145/3351095.3372840

Halaburda, H., Haeringer, G., Gans, J., & Gandal, N. (2018). *The Microeconomics of Cryptocurrencies* (Research Paper No. 2018-10–02). NYU Stern School of Business, Baruch College Zicklin School of Business. https://doi.org/10.2139/ssrn.3274331

Heilbroner, R. (1998). The self-deception of economics. *Critical Review*, *12*(1–2), 139–150. https://doi.org/10.1080/08913819808443490

Lotti, L. (2016). Contemporary art, capitalization and the blockchain: On the autonomy and automation of art's value. *Finance and Society*, *2*(2), 96. https://doi.org/10.2218/finsoc.v2i2.1724

Mirowski, P., & Nik-Khah, E. (2018). *The Knowledge We Have Lost In Information – The History Of Information in Modern Economics*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190270056.001.0001

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf

Nik-Khah, E., & Mirowski, P. (2019). On Going the Market One Better: Economic Market Design and the Contradictions of Building Markets for Public Purposes. *Economy and Society*, *48*(2), 268–294. https://doi.org/10.1080/03085147.2019.1576431

Ossandón, J. (2019). Notes on Market Design and Economic Sociology. *Economic Sociology*, *20*(2), 31–39. http://hdl.handle.net/10419/200967

Swartz, L. (2018). What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. *Cultural Studies*, *32*(4), 623–650. https://doi.org/10.1080/09502386.2017.1416420

Titcomb, A. (2019). Deep Dive: Augmented Bonding Curves [Blog post]. *Giveth Medium*. https://medium.com/giveth/deep-dive-augmented-bonding-curves-3f1f7c1fa751

Virtanen, A., Lee, B., Wosnitzer, R., & Bryan, D. (2018). Economics Back into Cryptoeconomics [Blog post]. *Econaut Medium*. https://medium.com/econaut/economics-back-into-cryptoeconomics-20471f5ceeea

Voshmgir, S. (2019). *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*. BlockchainHub Berlin.

Voshmgir, S., & Zargham, M. (2019). *Foundations of Cryptoeconomic Systems* [Working Paper]. Institute for Cryptoeconomics, Vienna University of Economics and Business. https://epub.wu.ac.at/7309/

Voskuill, E. (2018). *Cryptoeconomics* [Wiki Page]. The Bitcoin Development Library. https://github.com/libbitcoin/libbitcoin-system/wiki/Cryptoeconomics

Zamfir, V. (2015). *What Is Cryptoeconomics?* Cryptocurrency Research Group Cryptoeconomicon. https://youtu.be/9lw3s7iGUXQ?t=58

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

centre internet et societe

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya